(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－331181

(43)公開日　平成11年(1999)11月30日

| (51)Int.Cl.[6] | | 識別記号 | ＦＩ | | |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 12/28 | | Ｈ０４Ｌ | 11/00 | ３１０Ｚ |
| Ｇ０６Ｆ | 13/00 | ３５１ | Ｇ０６Ｆ | 13/00 | ３５１Ｚ |
| | 15/00 | ３３０ | | 15/00 | ３３０Ｂ |
| | | | | | ３３０Ｃ |
| Ｈ０４Ｌ | 9/32 | | Ｈ０４Ｌ | 9/00 | ６７３Ａ |

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願平10－130788

(22)出願日　平成10年(1998)５月13日

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号

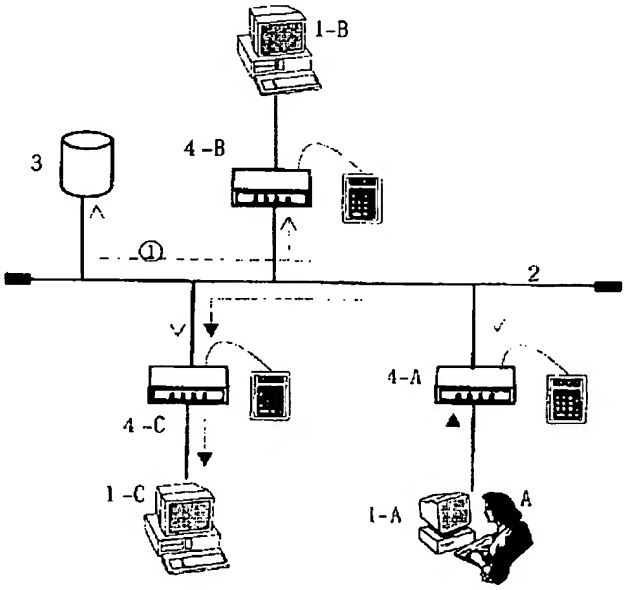
(72)発明者　北村　徹
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

(54)【発明の名称】　ネットワーク端末認証装置

(57)【要約】

【課題】正当でない端末のネットワークの利用を禁止するために、ネットワークを利用する全ての端末にネットワーク端末認証装置を介した通信を行うことにより、不正な端末及びユーザのネットワークの使用を防止することを目的とした。

【解決手段】　ネットワークに接続された端末及びこの端末を利用するユーザの認証を行うネットワーク端末認証装置であって、ネットワークに接続された端末とユーザを識別する識別手段と、ネットワーク利用許可されている端末とユーザを記憶した記憶手段と、識別手段により識別された端末及びユーザと、記憶手段の端末及びユーザとを比較する比較手段と、比較手段の結果によりネットワークの利用を禁止する制御手段とを備えたことを特徴とするネットワーク端末認証装置である。



1

【特許請求の範囲】

【請求項１】ネットワークに接続された端末及びこの端末を利用するユーザの認証を行うネットワーク端末認証装置であって、ネットワークに接続された端末とユーザを識別する識別手段と、ネットワーク利用許可されている端末とユーザを記憶した記憶手段と、上記識別手段により識別された端末及びユーザと、上記記憶手段の端末及びユーザとを比較する比較手段と、上記比較手段の結果によりネットワークの利用を禁止する制御手段と、を備えたことを特徴とするネットワーク端末認証装置。

【請求項２】上記記憶手段は、ネットワークに接続可能な情報である端末情報、ネットワークの利用可能ユーザの情報であるユーザ情報、ネットワークに接続された端末を利用することができる端末利用ユーザ情報を連携して管理することを特徴とする請求項１に記載されたネットワーク端末認証装置。

【請求項３】上記機能を持ったネットワーク端末認証装置間でしか通信が行えない機能を有することを特徴とする請求項１または請求項２に記載されたネットワーク端末認証装置。

【請求項４】上記ネットワーク端末認証装置間では暗号化されたものが通信されることを特徴とする請求項１ないし請求項３に記載されたネットワーク端末認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークに接続する端末及びこの端末を利用するユーザを管理する技術に関し、特に正当に使用許可を得られていない端末及びユーザを、構築されたネットワーク環境内に自由に接続して通信をすることを禁止し、ネットワーク内のセキュリティを高める技術に関するものである。

【０００２】

【従来の技術】従来、ユーザが端末をネットワークに接続して利用する場合、ネットワークに構成するＥｔｈｅｒｎｅｔケーブルや、光ケーブルなどに自由に端末を接続することが可能である。その結果、ネットワーク上に自由にパケットを流すことができ、接続された端末と自由に通信することが可能である。以下、図面を用いて従来技術を説明する。図１は従来のネットワークの認証の構成を示す図面である。図１において、Ａはコンピュータシステムの端末を利用するユーザであり、１－Ａ、１－Ｂ、１－Ｃはパーソナルコンピュータゆあワークステーションなどの端末であり、ネットワーク通信を可能とするＬＡＮ接続装置を含んだものであり、ユーザはこれらの端末を利用しネットワークに接続することができる。２はネットワークを形成するための物理的媒体となる銅線や光ケーブルであり、３はユーザのネットワーク利用情報、具体的にはユーザＩＤやユーザのグループＩＤのようなユーザ等を記憶するための記憶装置である。

2

ネットワークの利用の仕方は、例えば、ユーザＡが端末１－Ａをネットワーク２に接続した時、ユーザＡの認証を端末１－Ａから記憶装置３に問い合わせ、ネットワーク利用の許可を得て、ネットワーク２を利用する。つまり、ネットワークに接続された端末（１－Ｂ、１－Ｃなど）と自由に通信することが可能となる。

【０００３】

【発明が解決しようとする課題】しかしながら、ネットワークに接続することが可能であると、全てのユーザが自由に端末をネットワーク内に接続するとこが可能となり、ネットワークの使用許可が行われていない不正な端末でもネットワークを用いての通信が可能となるので、不正なユーザが正当なユーザへのなりすましや、不正な端末接続によるデータ伝達の障害を招く可能性が高まり、ネットワーク自体の正当性が保証されなくなってしまう。本発明は上記課題を解決するためになされた発明であり、正当でない端末のネットワークの利用を禁止するために、ネットワークを利用する全ての端末にネットワーク端末認証装置を介した通信を行うことにより、不正な端末及びユーザのネットワークの使用を防止することを目的とした発明である。

【０００４】

【課題を解決するための手段】本発明の請求項１に記載された発明は、ネットワークに接続された端末及びこの端末を利用するユーザの認証を行うネットワーク端末認証装置であって、ネットワークに接続された端末とユーザを識別する識別手段と、ネットワーク利用許可されている端末とユーザを記憶した記憶手段と、上記識別手段により識別された端末及びユーザと、上記記憶手段の端末及びユーザとを比較する比較手段と、上記比較手段の結果によりネットワークの利用を禁止する制御手段とを備えたことを特徴とするネットワーク端末認証装置である。また、請求項２に記載されは発明は、上記記憶手段は、ネットワークに接続可能な情報である端末情報、ネットワークの利用可能ユーザの情報であるユーザ情報、ネットワークに接続された端末を利用することができる端末利用ユーザ情報を連携して管理することを特徴とする請求項１に記載されたネットワーク端末認証装置である。また、請求項３に記載された発明は、上記機能を持ったネットワーク端末認証装置間でしか通信が行えない機能を有することを特徴とする請求項１または請求項２に記載されたネットワーク端末認証装置である。また、請求項４に記載された発明は、上記ネットワーク端末認証装置間では暗号化されたものが通信されることを特徴とする請求項１ないし請求項３に記載されたネットワーク端末認証装置である。

【０００５】具体的には、ネットワーク端末認証装置におけるネットワークに接続可能な端末の識別手段は、ＩＳＯにより定められたＩＳＯ参照モデルで示されるデータリンク層（第２層）レベルで認証を行う。例えば、端

末を識別するために与えられたＬＡＮ接続装置の一意な番号を基に端末の認証を行う。また、この認証の際に伝達するデータはセキュリティを確保するために、ＤＥＳなどによる暗号化の処理を行う。この結果、ユーザの認証はパスワードによる入力やＩＣカード入力による情報を処理できる。また、ネットワーク上に接続された端末同士の通信は、ネットワーク端末認証装置同士がデータを上記した暗号化及び複合化して送受信する方法を用いる。ネットワーク端末認証装置は、ネットワーク端末認証装置同士以外とは通信を行うことができず、ネットワークに接続される端末は、ネットワーク端末認証装置を介した通信を行うことなり、認証データベースに登録されていない端末及びユーザの利用を禁止することが可能となる。つまり、通信中データを暗号化しているため、ネットワーク端末認証装置でしか通信が行えない。また、ネットワーク端末認証装置ないにデータベースを設置すると汎用性がなくなるために、ネットワーク端末認証装置とデータベースが独立して設定されている。また、ネットワーク端末認証装置とデータベースの間で通信されるデータは、暗号化されていてもされていなくとも良いものとする。

【０００６】

【発明の実施の形態】以下、図面を用いて本発明を具体的に説明する。図２は本発明のネットワーク端末認証装置のネットワーク端末の認証の実施形態を表す図面であり、図３はネットワーク認証端末装置のデータの流れを示すフローチャートである。図２において、Ａは端末を利用するユーザであり、１－Ａ、１－Ｂ、１－Ｃはパーソナルコンピュータやワークステーションなどの端末であり、ネットワーク通信を可能とするＬＡＮ接続装置を含んだものであり、ユーザＡはこれらの端末を利用しネットワークに接続する。２はネットワークを形成するための物理的媒体となる銅線や光ケーブルであり、３はユーザのパスワードやＩＣカードなどのユーザを特定する情報と、ネットワークを接続する端末を一意に決定するために与えられた番号を管理している。例えば、ネットワークカードに割り当てられた、４８ビットで表されるＭＡＣアドレスであり、さらに、個々の端末を利用できるユーザの情報を管理した記憶装置である。４はネットワーク端末であり、ユーザ情報の入力のためのテンキーやＩＣカード読み取り装置などの入力装置を具備している。

【０００７】また、図５、図６はネットワーク端末認証装置に接続可能な端末を識別するために与えられた一意なＭＡＣアドレスのような番号、ならびにネットワーク認証装置を利用可能なユーザＩＤを蓄積してデータベース構造の例である。

【０００８】次に、図３に示されているフローチャートを用いて、ネットワーク端末認証装置の通信処理の流れを説明する。まず、ユーザＡは端末１－Ａをネットワーク上に接続する際、ネットワーク端末認証装置４を介して端末１－Ａをネットワーク２に接続する（ステップ１）。次いで、ユーザＡはネットワーク端末認証装置４－Ａにユーザ情報を入力する（ステップ２）。入力されたユーザ情報は、ネットワーク端末認証装置のＩＤ番号など、ネットワーク端末認証装置と接続された端末のＭＡＣアドレス情報などの各情報はネットワーク端末認証装置により暗号化されて、記憶装置３にネットワークを用いて通信される。上記ネットワーク端末認証装置４－Ａと記憶装置３に付随している通信制御手段は、ＯＳＩの７階層中の第２層レベル（データリンク層）にプロトコルで通信される。そして、記憶装置３に伝達された上記各情報を図５、図６に示されるようなデータベースに記憶されている対象データと、ネットワーク端末認証装置、ネットワーク端末認証装置に接続された１－ＡのＬＡＮ接続装置に接続された一意な番号ならびに端末を利用するユーザＡの情報とを対比させることにより認証を行う（ステップ４）。この認証の結果、ネットワーク利用が禁止されていれば、１－Ａに接続されたネットワーク端末認証装置は、１－Ａから受け取る通信データを全て廃棄し、ネットワーク上にデータを流さないようにする（ステップ５）。また、認証の結果、ネットワークの利用が許可されれば、端末１－Ａからネットワーク端末認証装置へ送られるデータを暗号化し、ネットワーク上に接続された端末との通信を可能にする（ステップ６）。以上のような処理が行われて、本発明のネットワーク端末認証装置のデータの流れは終了する。

【０００９】次いで、ネットワークに接続された端末１－Ａと端末１－Ｂの通信のやり方を説明する（図４参照）。図４において、Ａは端末を利用するユーザ、１－Ａ、１－Ｂはパーソナルコンピュータやワークステーションなどの端末であり、ネットワーク通信を可能にするＬＡＮ接続装置を含んだものであり、ユーザはこれらの端末を利用しネットワークを利用する。２はネットワークを形成するための物理的媒体となる銅線や光ケーブルであり、３はパスワードやＩＣカードなどのユーザを特定する情報と、ネットワークを接続する端末を一意に決定するために与えられたＭＡＣアドレスなどの番号の情報を管理し、さらに個々の端末を利用できるユーザ情報を管理した記憶装置であり、４はネットワーク端末認証装置であり、ユーザ情報の入力のためのテンキーやＩＣカード読みとり装置などの入力装置を具備している。また、ａ、ｂは端末１－Ａ、端末１－ＢのＬＡＮ装置に与えられた一意のＭＡＣアドレスである。

【００１０】以下に、ネットワークに接続された端末１－Ａと端末１－Ｂの通信の状態を詳細に図面を用いて説明する（図４参照）。端末１－Ａから端末１－Ｂへの通信では、まず、ネットワーク端末認証装置４－Ａが端末１－Ａから受け取ったデータをもとに端末１－ＡのＭＡＣアドレスａと通信相手の端末１－ＢのＭＡＣアドレス

5

bを取り出し、記憶装置３にネットワークの利用を問い合わせる。問い合わせの結果、端末１－Ａと端末１－Ｂがネットワークにより通信できるならば、端末１－Ａから受信したデータを暗号化し、端末１－Ｂが接続されたネットワーク端末認証装置４－Ｂへ暗号化されたデータを送信する。このネットワーク端末４－Ｂは、受け取った暗号化されたデータを複合化して端末１－Ｂへ送信する。記憶装置３の問い合わせで通信が許可されない場合は、ネットワーク端末認証装置１－Ａで受け取ったデータを破棄する。したがって、ネットワーク端末認証装置を介さないでネットワークが接続され、他の端末と通信しようとしても、ネットワーク端末認証装置同士の通信は確立しないためネットワーク端末認証装置では通信を実現することはできない。

【００１１】

【発明の効果】以上のように、本発明のネットワーク端末認証装置では、正当にネットワークの使用許可を受けていない端末のネットワーク接続、及びユーザのネットワークの利用を禁止することができ、ネットワーク上のセキュリティを高めることができる。また、ネットワーク接続可能な端末ならびに、ネットワークを利用できるユーザ、ネットワークに接続された端末を利用できることができるユーザを統一的に管理することができる。また、ネットワーク上に接続される端末は、ネットワーク

6

上でネットワーク端末認証装置を介して通信することで、不正なネットワーク上の通信を排除することができ、また暗号化されたデータ通信によりネットワークの盗聴によるデータの漏洩などを防止することができる。

【図面の簡単な説明】

【図１】従来のネットワークシステムを示す概略図である。

【図２】本発明のネットワーク端末認証装置のネットワーク端末の認証の状態を示す概略図。

【図３】本発明のネットワーク端末認証装置でのデータの流れを表したフローチャートである。

【図４】本発明のネットワーク端末認証装置間で通信を行う際のネットワーク端末の認証の状態を示す概略図である。

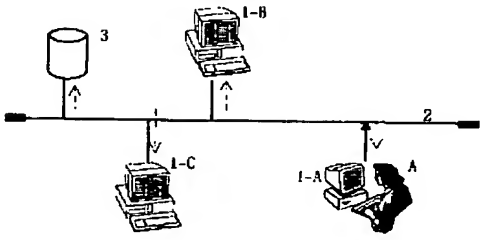
【図５】本発明のネットワーク端末認証装置に接続可能な端末を識別するために用いられるデータサーバ構造の例である。

【図６】本発明のネットワーク端末認証装置に接続可能な端末を識別するために用いられるデータサーバ構造の例である。

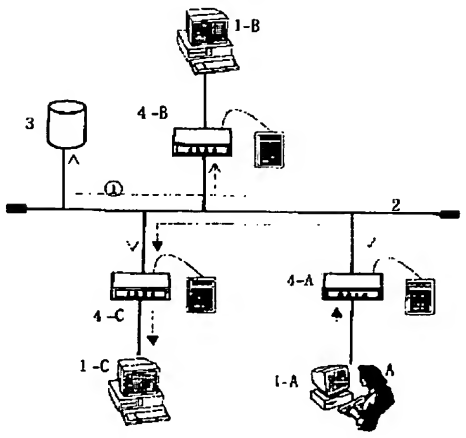
【符号の説明】

１…端末　２…ネットワーク　３…記憶装置　４…ネットワーク端末認証装置

【図１】




【図２】



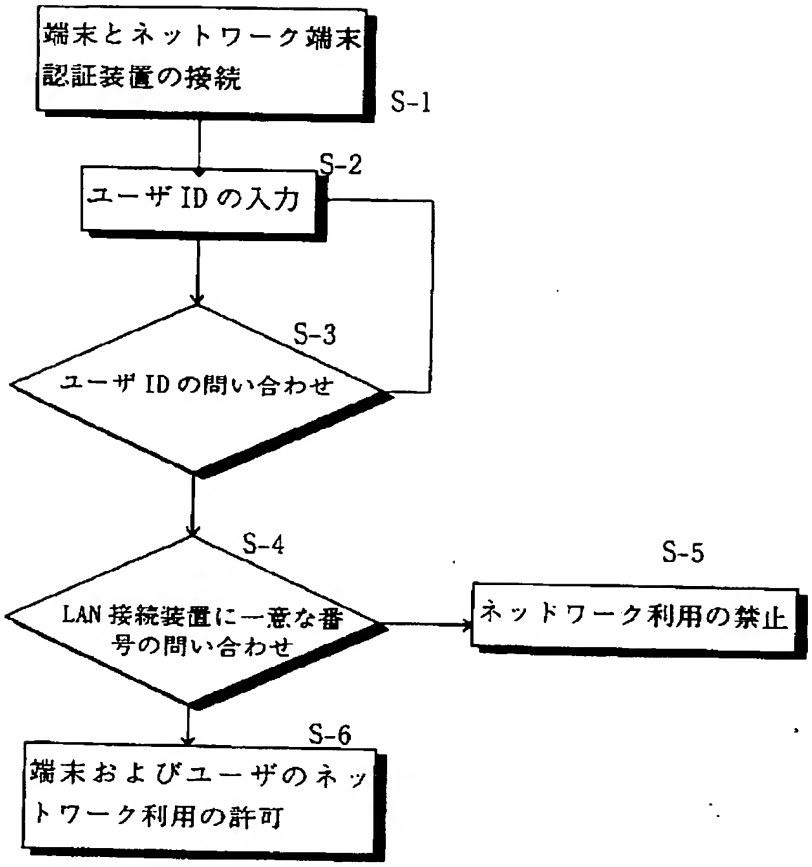

【図５】

| ネットワーク接続可能端末 | LAN接続装置に一意な番号 |
|---|---|
| ネットワーク端末認証装置Ａ | 00:AA:BB:CC:DD |
| | 00:AA:11:22:33 |
| ネットワーク端末認証装置Ｂ | 00:AA:BB:CC:EE |
| | 00:BB:AA:22:33 |
| | 00:CC:22:33:44 |
| ネットワーク端末認証装置Ｂ | 00:AA:BB:CC:EE |

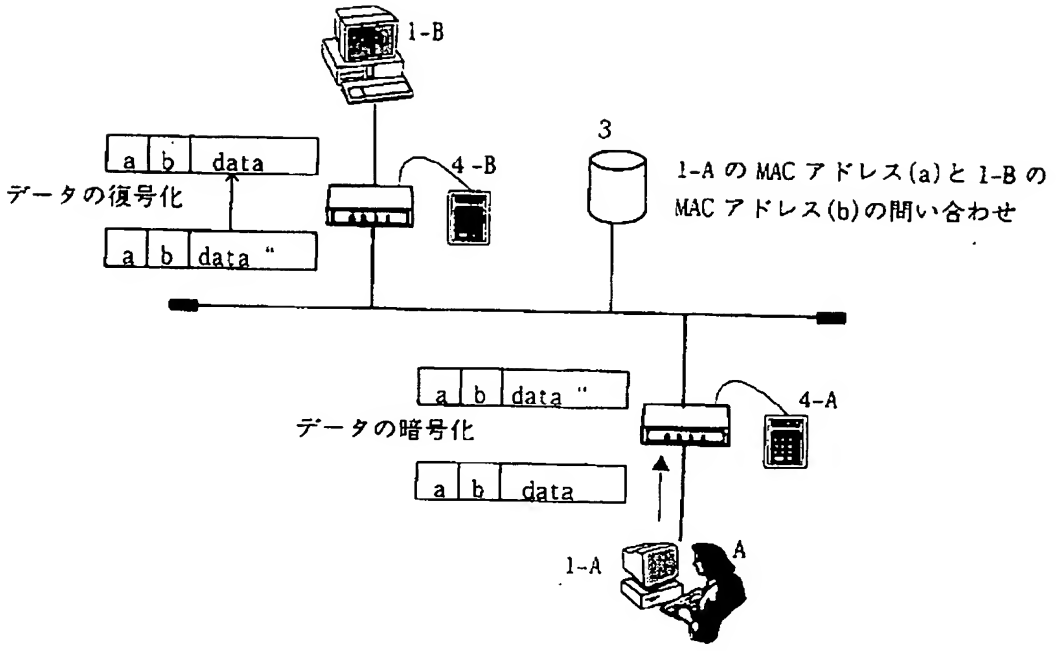
【図６】

| ネットワーク接続可能端末 | ユーザーID |
|---|---|
| ネットワーク端末認証装置Ａ | 0000001 |
| | 0000033 |
| | 0002380 |
| ネットワーク端末認証装置Ｂ | 0000002 |
| ネットワーク端末認証装置Ｃ | 0000015 |

【図３】



【図４】




フロントページの続き

| (51) Int. Cl.[6] | 識別記号 | F I |
|---|---|---|
| | | H０４L　9/00　　６７３B |